資訊安全實習 ①

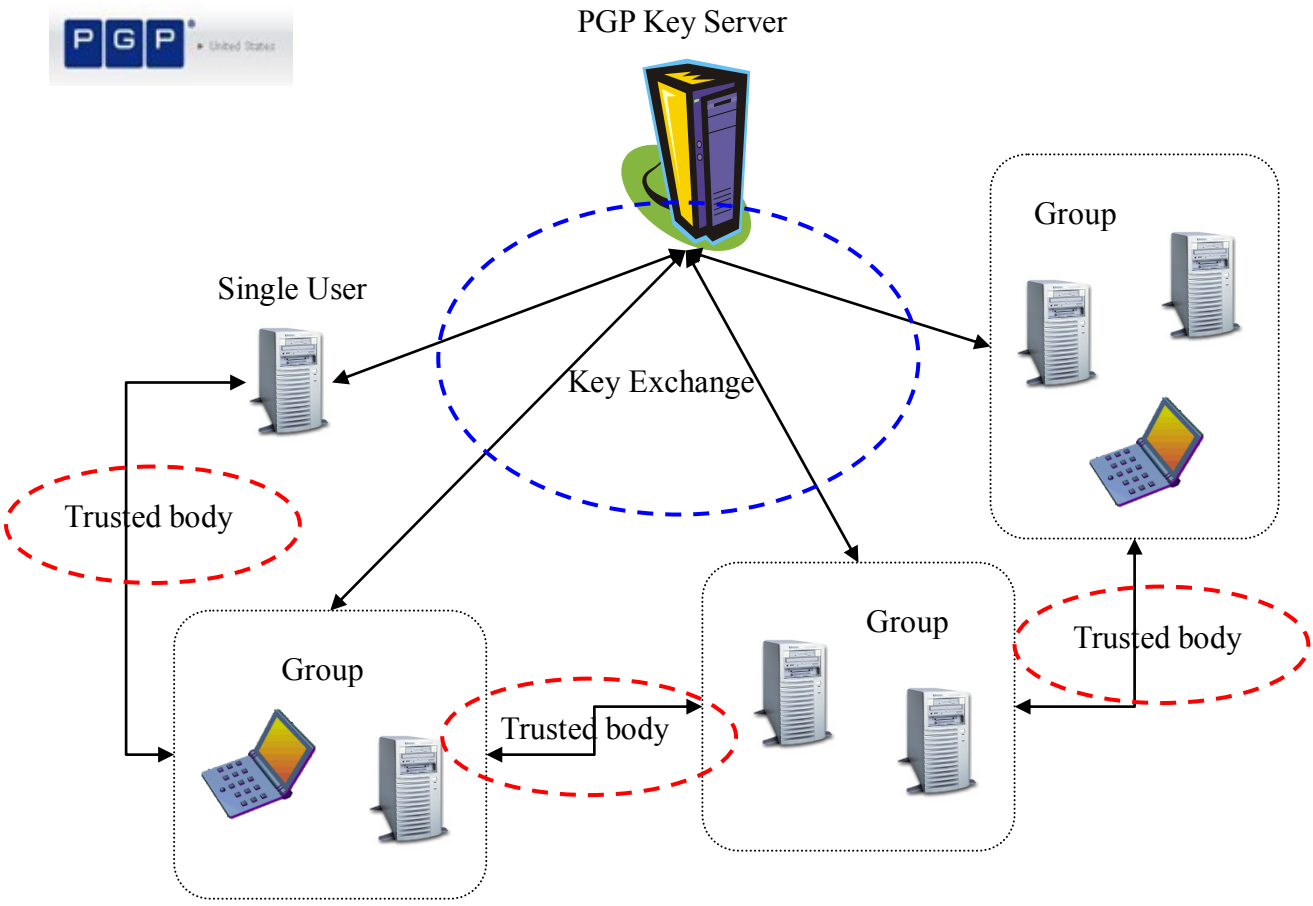
實驗名稱 － ＰＧＰ(Pretty Good Privacy)

本實驗之目的主要讓學員瞭解軟體 PGP 安裝與操作，以及與公私鑰密碼學相關之背景實際操作。學員可由安裝過程中瞭解非對稱密碼學實際運用之流程以及對現有密碼相關軟體有一定程度之認識。

實驗所需背景

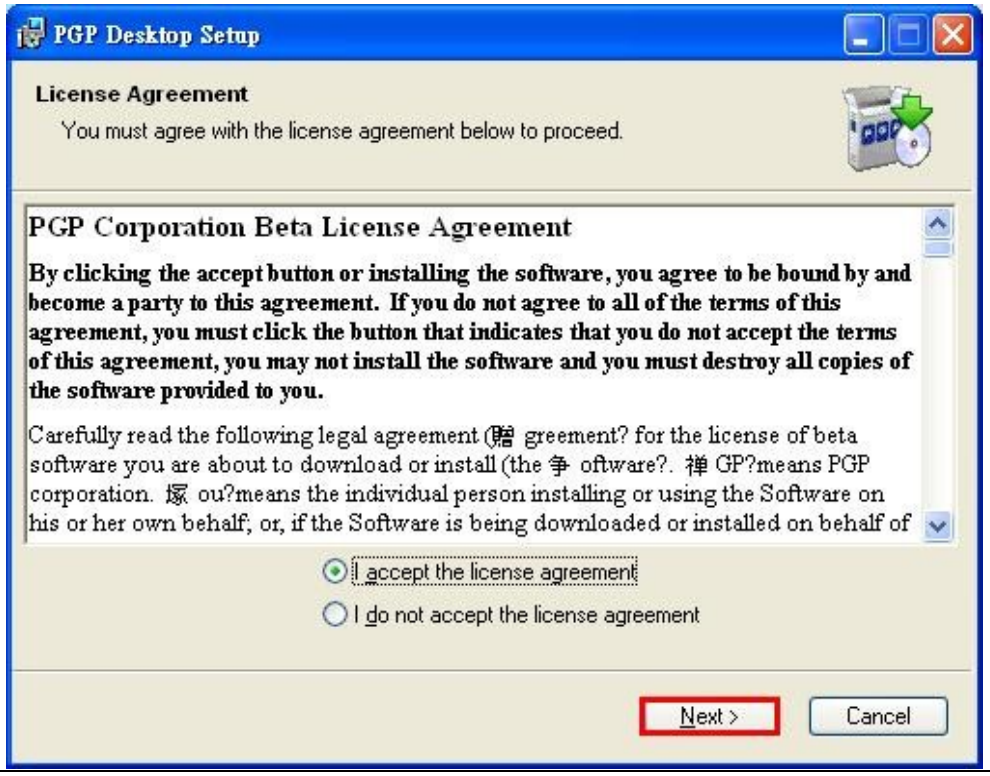
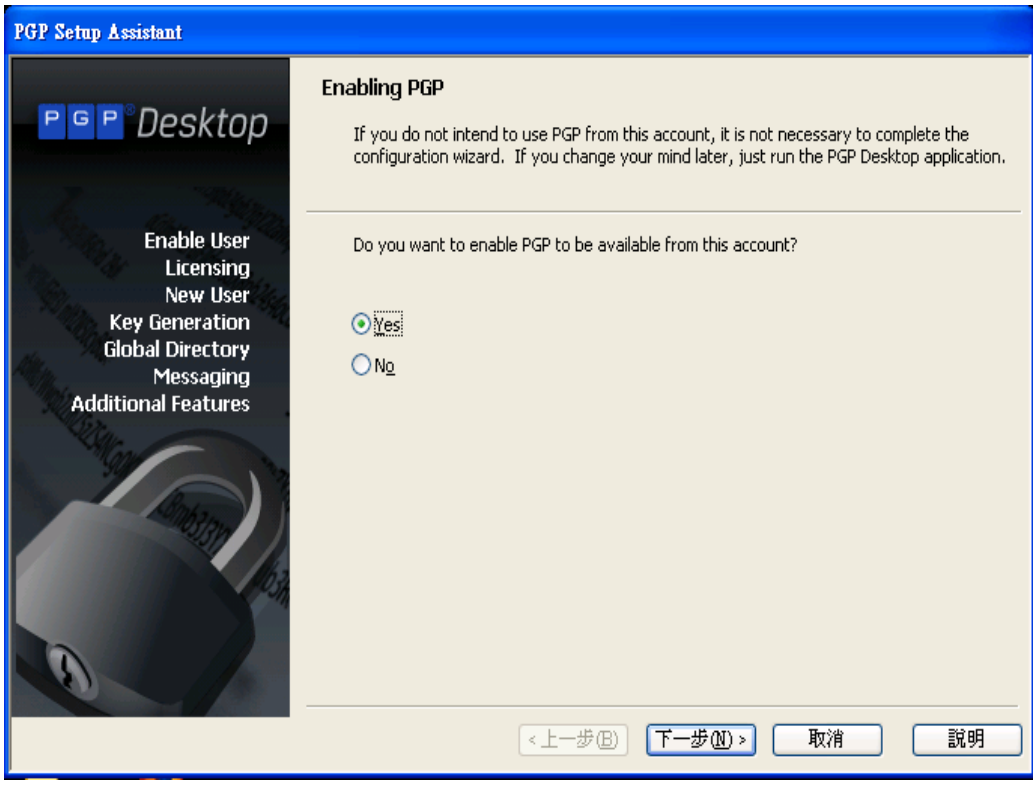
學員需具有非對稱密碼學之基礎背景知識，以及電腦軟體安裝與操作之基礎能力。

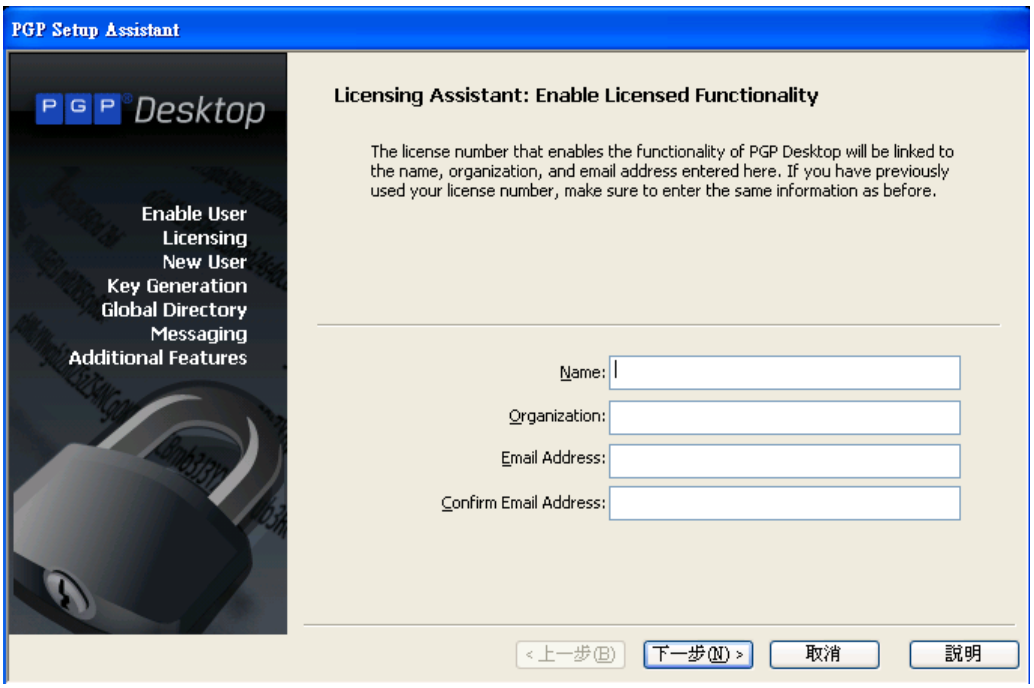
實驗示意圖

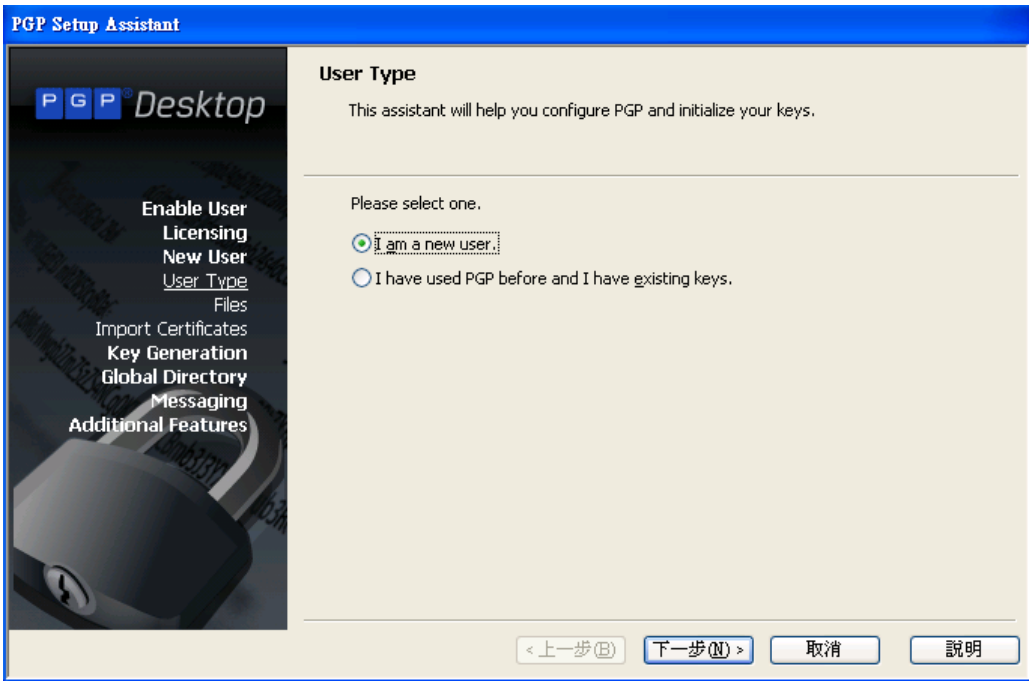
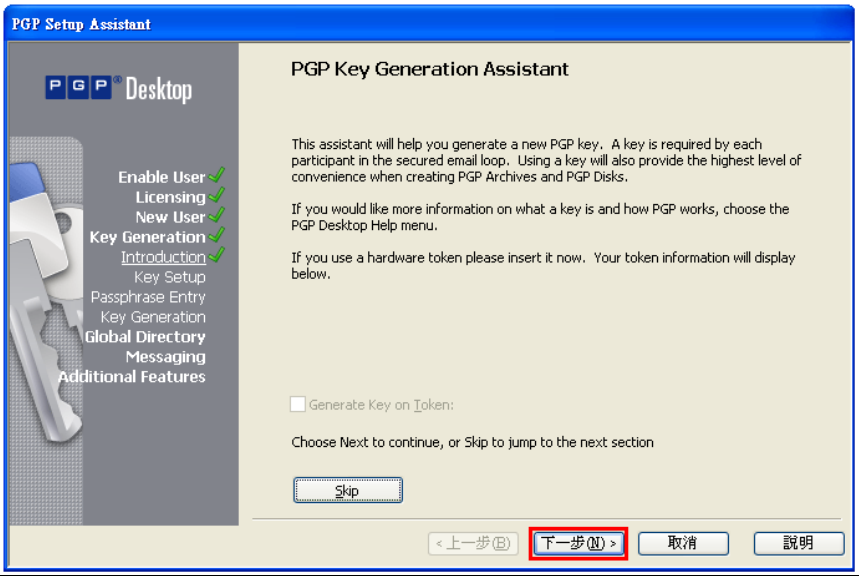


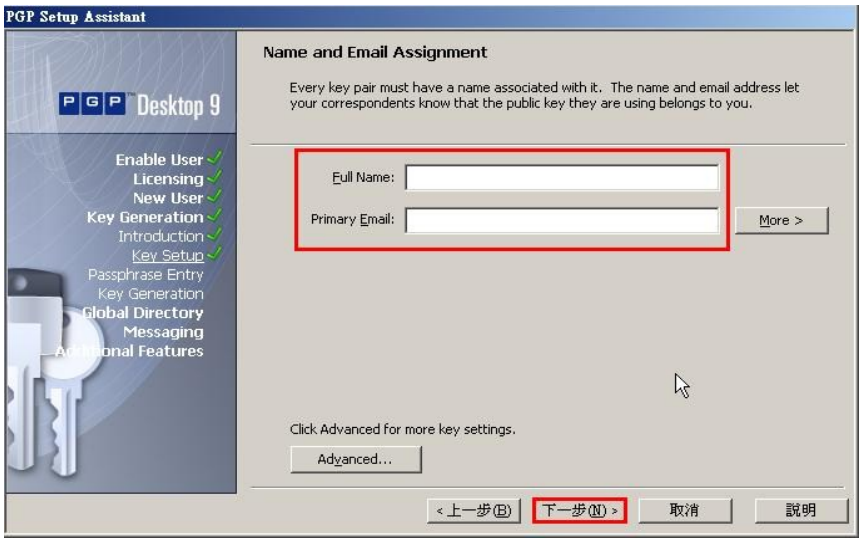
實驗測試步驟

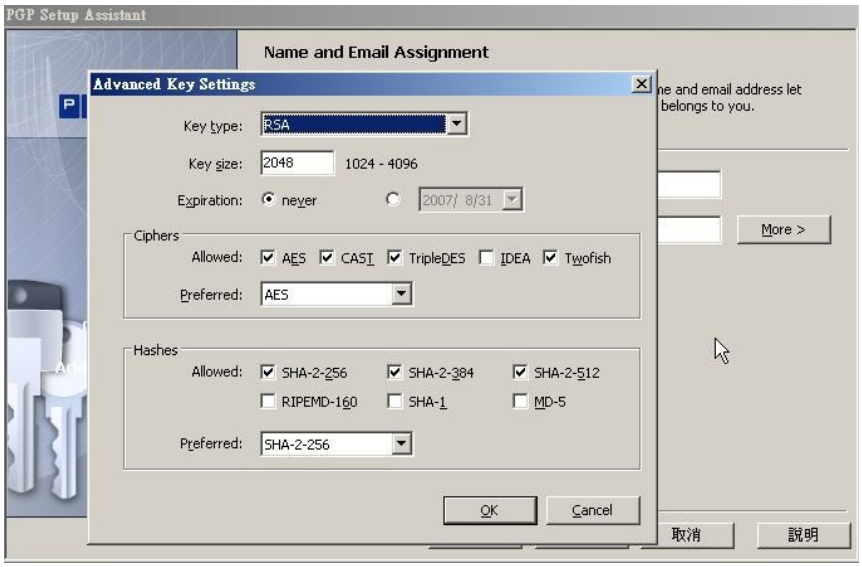
1. PGP Desktop 安裝並設定

Step 1	請至網站下載壓縮檔，解壓縮後，執行 PGPDesktopWin32-10.1.1.exe 安裝檔，選擇用 English 語系安裝，在下面的界面點選 I accept the license agreement 後即可選擇 Next。 
Step 2	之後再按 Next 即開始安裝，安裝完後會要求重開機。重開機完後即開始 PGP 軟體設定。重開機後所開啟的設定視窗，一開始選擇 Yes 並按下一步。 

Step 3	這邊則在讓使用者資料填寫資料，使用者:Trial User 組織:30 Day Product Trial，email 留下空白，如果之前有註冊過 PGP 之前的版本，則要填和之前一樣的資料。 
Step 4	確認使用者及組織過後的畫面 

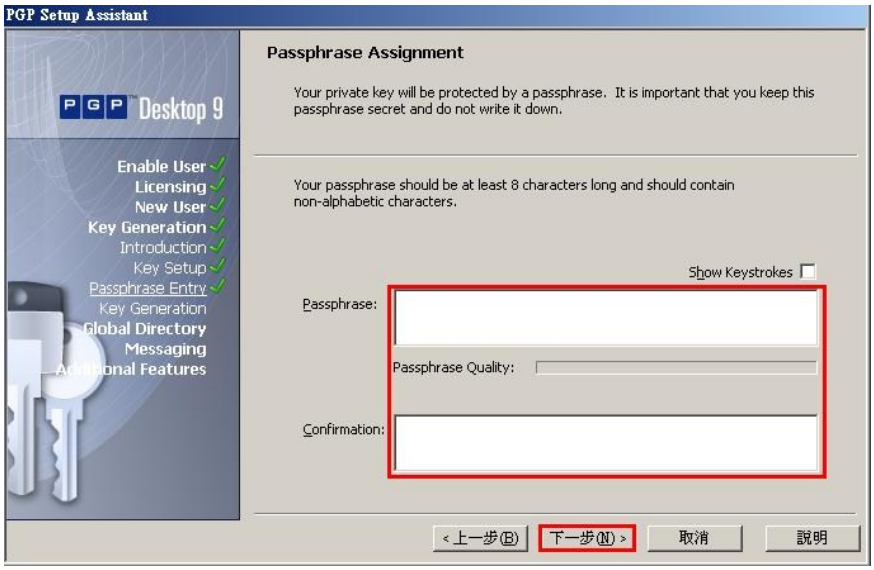
Step 5	接下來則確認使用者有無用過 PGP 產品，如果有用過，則可以匯入之前的金鑰，如果沒有，則選擇為新的使用者就可以了。 
Step 6	在這步驟產生新的金鑰，需輸入 Full Name (統一用學號作為 Full Name) 以及要與 PGP 連結的 Email 信箱(學校信箱)，而選擇下方的 Advanced 則可以進入金鑰的詳細設定，如加密演算法，長度等，這邊我們皆以預設為主。填完所有資訊後選擇下一步。 

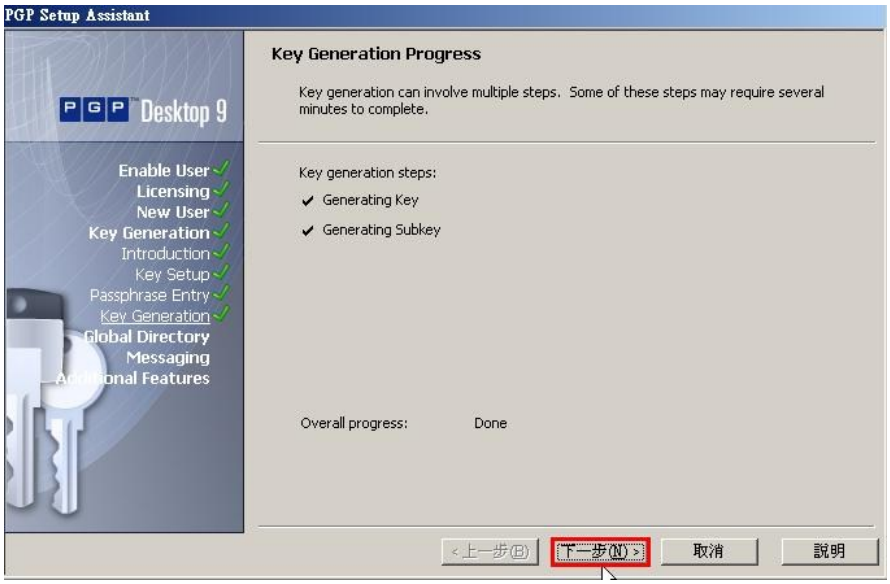
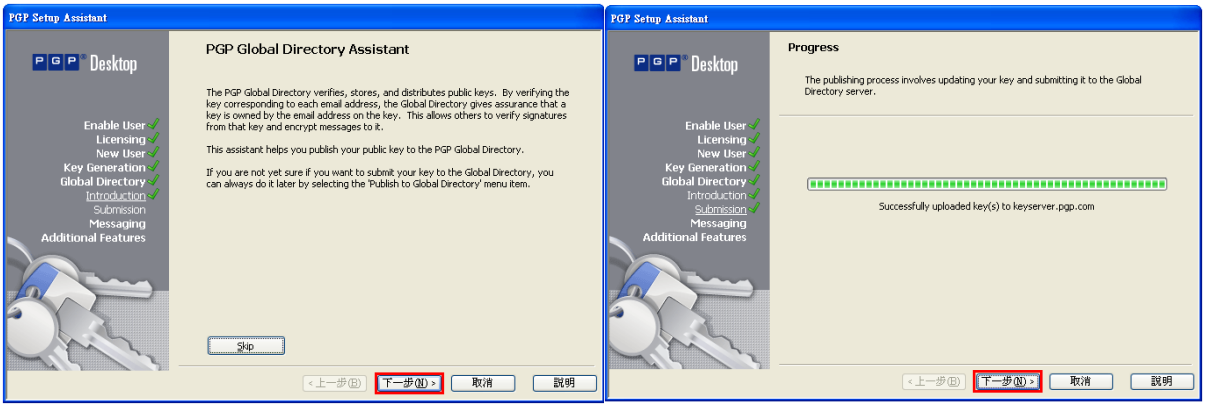
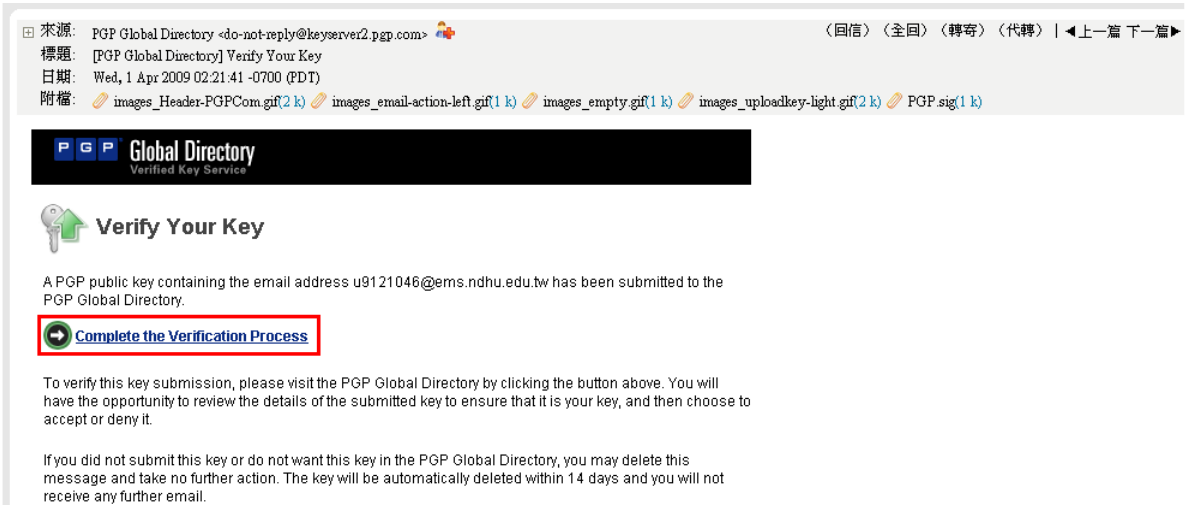




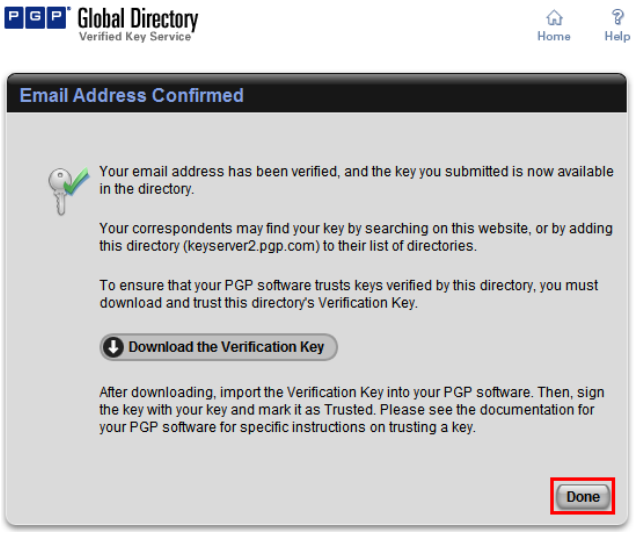
Step 7

由於所產生出來的私密金鑰非常長且難記，因此需要使用者輸入容易記憶的通行片語，來保護此私密金鑰。另外在輸入通行片語的過程中，中間會顯示此通行片語的強度。Show Keystrokes 選項勾選的話，則會顯示使用者出入的字元。

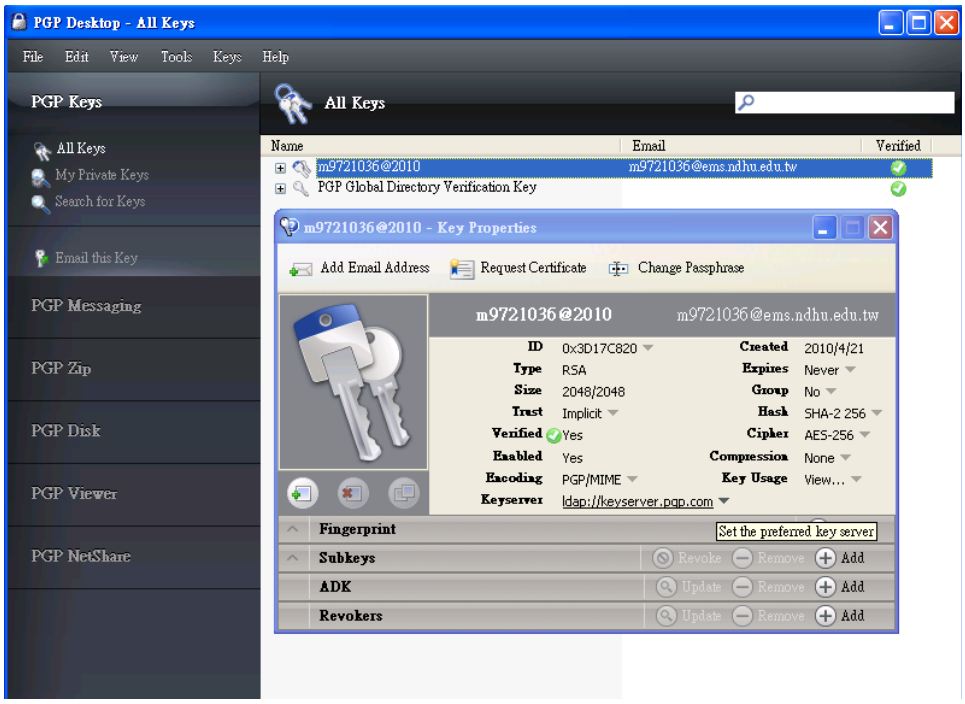
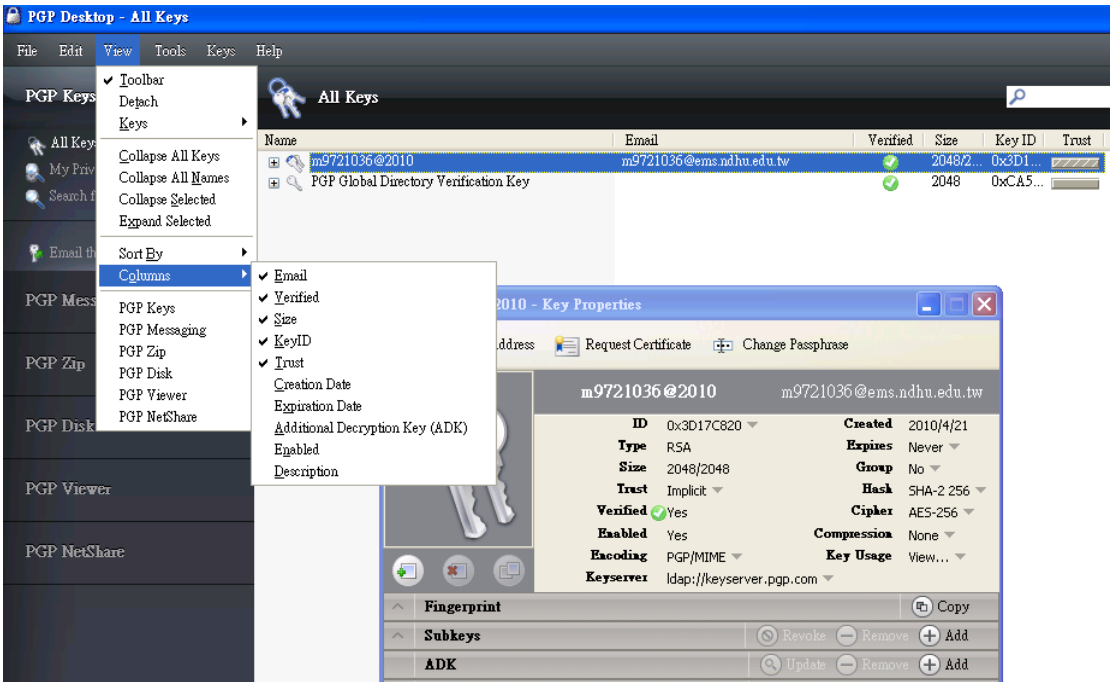


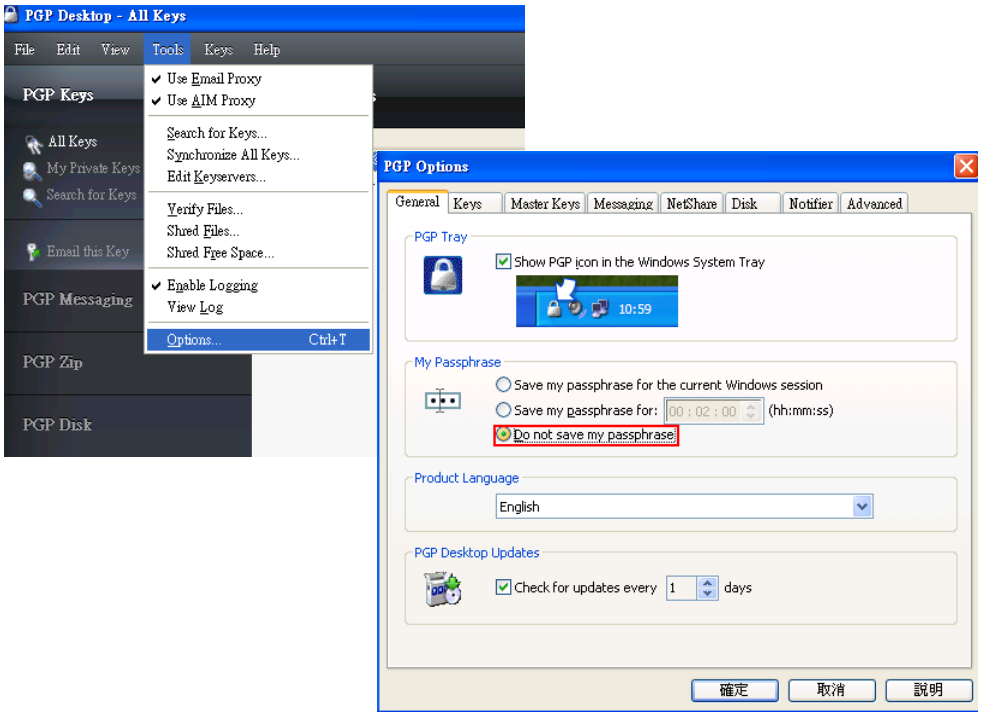
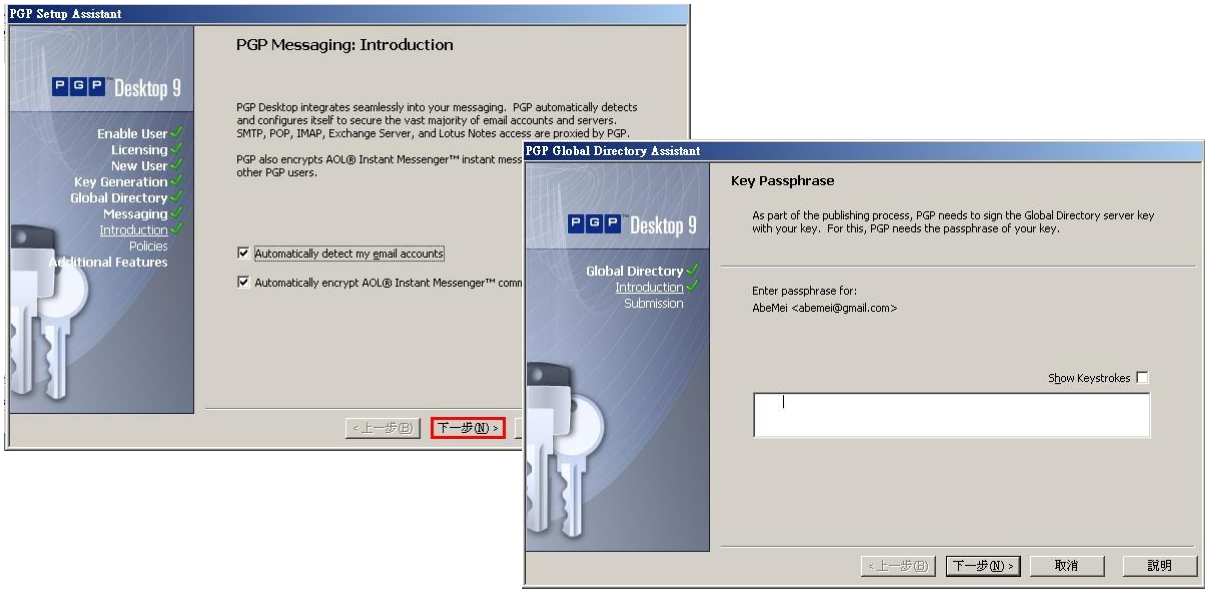
Step 8	產生金鑰完成後即可按下一步。 
Step 9	在這個步驟裡，我們將會把剛剛產生的公開金鑰公佈到 PGP 的 Key sever 上 (keyserver.pgp.com)，按下一步即會把你的公開金鑰上傳。 
Step10	請開啟信箱收信，會有一封要求你驗證公開金鑰的信件，點下 Complete the Verification Process 即會開啟一個驗證網頁，確認網頁的資料無誤後點選 Accept，再點選下一個網頁的 Done 即可完成 Key 的上傳與驗證。 

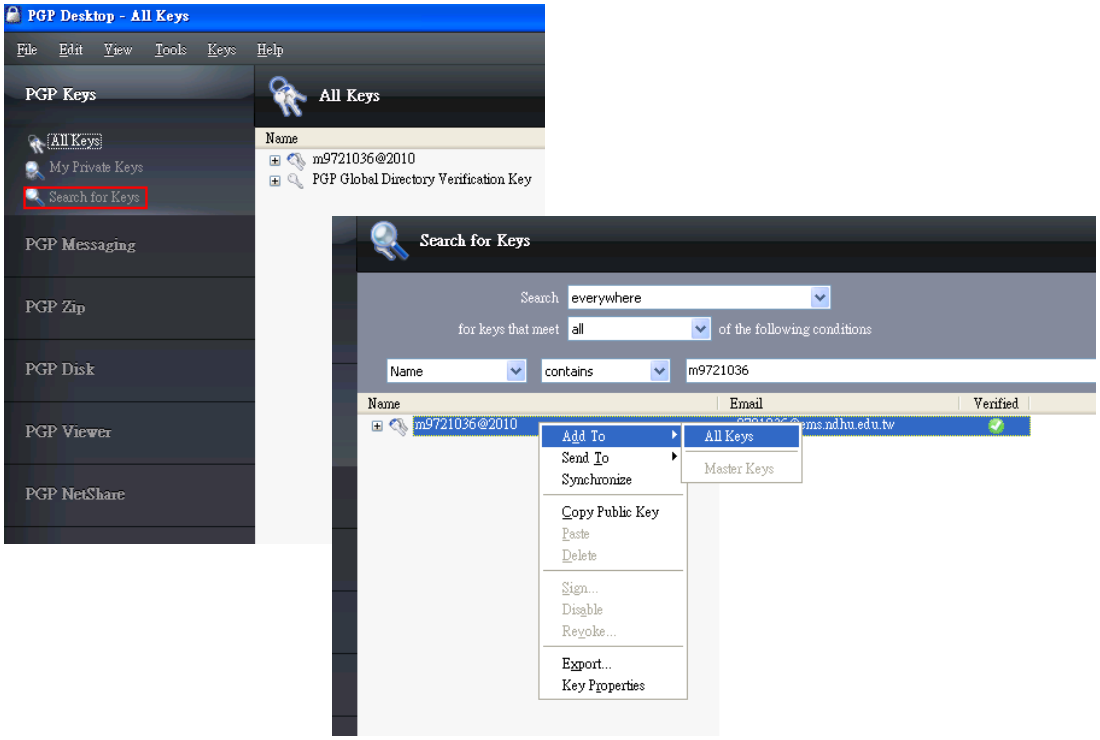
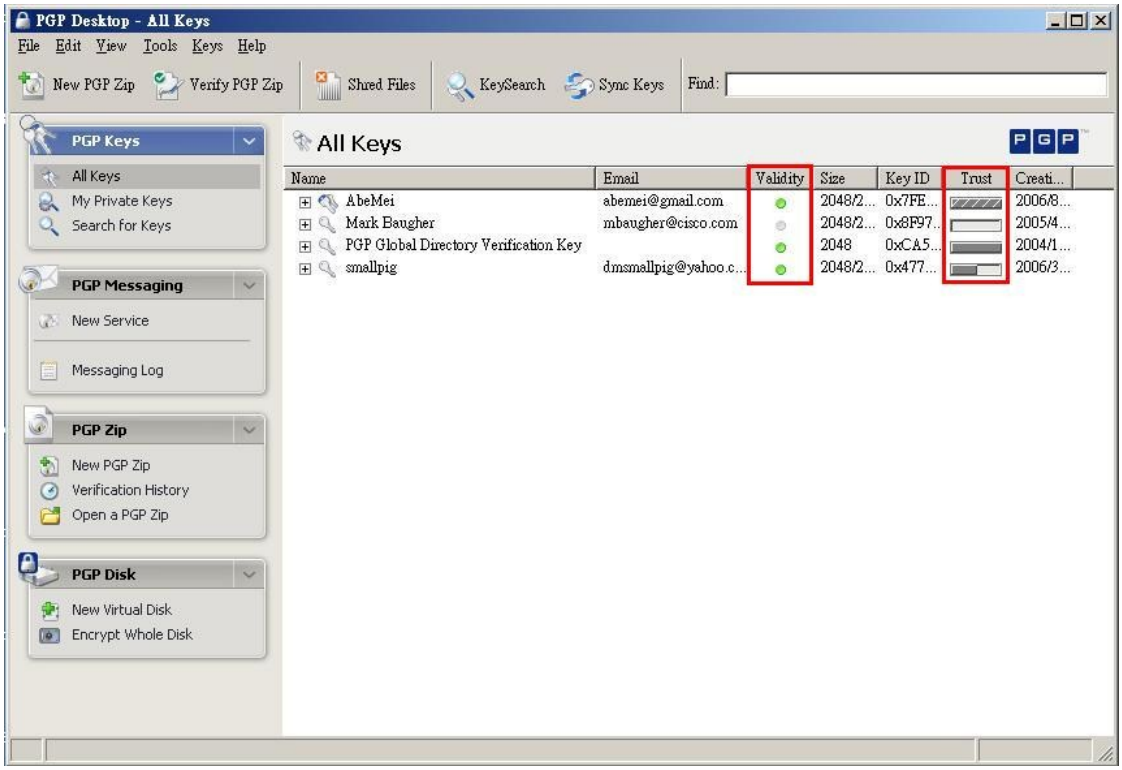

PGP Global Directory
Verified Key Service
Home
Help
Verify Your Key
49121046
0xAEF188BB
009C 0B30 35B2 B733 8101
A714 5AA4 921B AEF1 88BB
hihiwhen@gmail.com
0 signatures from other users
The PGP public key shown above has been submitted to the directory.
If you did not submit this key or you do not want this key in the directory, click 'Cancel'. The key will be deleted and you will not receive any further email regarding it.
Your email address hihiwhen@gmail.com is one of those attached to the key with the fingerprint shown above. If the key published for you is not yours, you will not be able to decrypt messages sent to you. If the fingerprint matches, and you want to publish the key for this address, click 'Accept'. Other PGP users will then be able to retrieve it in order to encrypt messages to you and verify signed messages from you.
Cancel
Accept

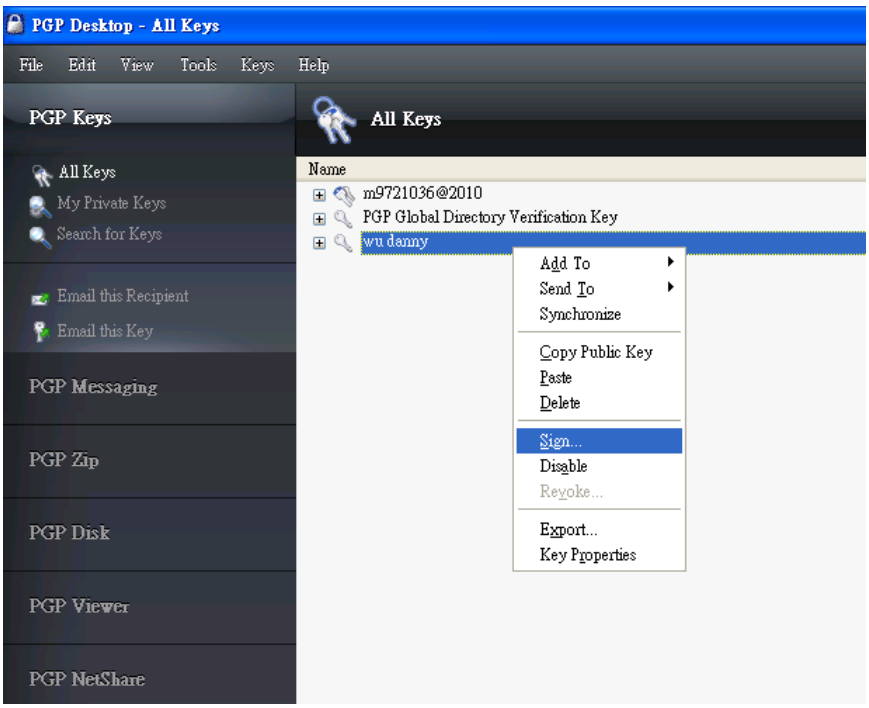
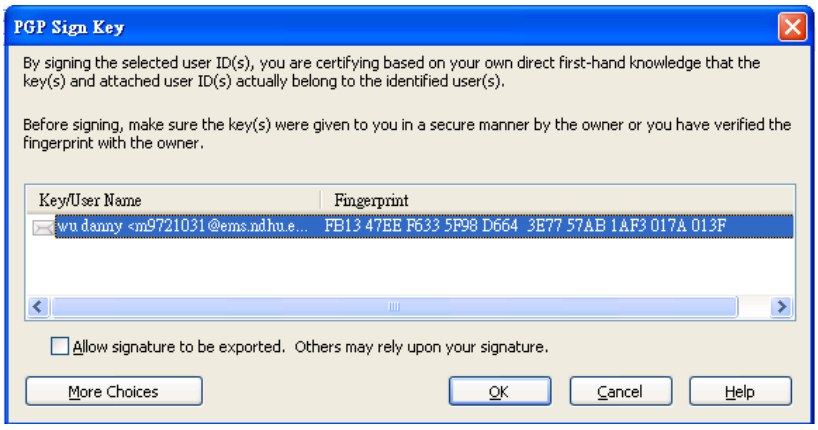
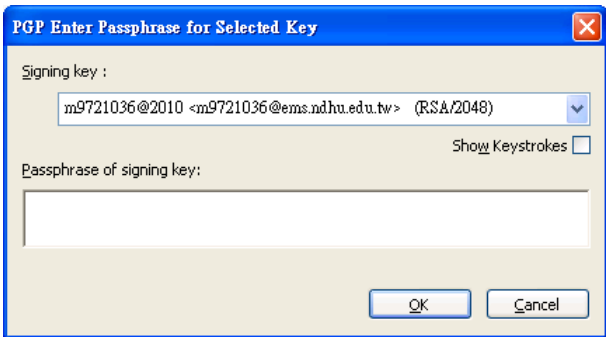

PGP Global Directory
Verified Key Service
Home
Help
Email Address Confirmed
Your email address has been verified, and the key you submitted is now available in the directory.
Your correspondents may find your key by searching on this website, or by adding this directory (keyserver2.pgp.com) to their list of directories.
To ensure that your PGP software trusts keys verified by this directory, you must download and trust this directory's Verification Key.
Download the Verification Key
After downloading, import the Verification Key into your PGP software. Then, sign the key with your key and mark it as Trusted. Please see the documentation for your PGP software for specific instructions on trusting a key.
Done

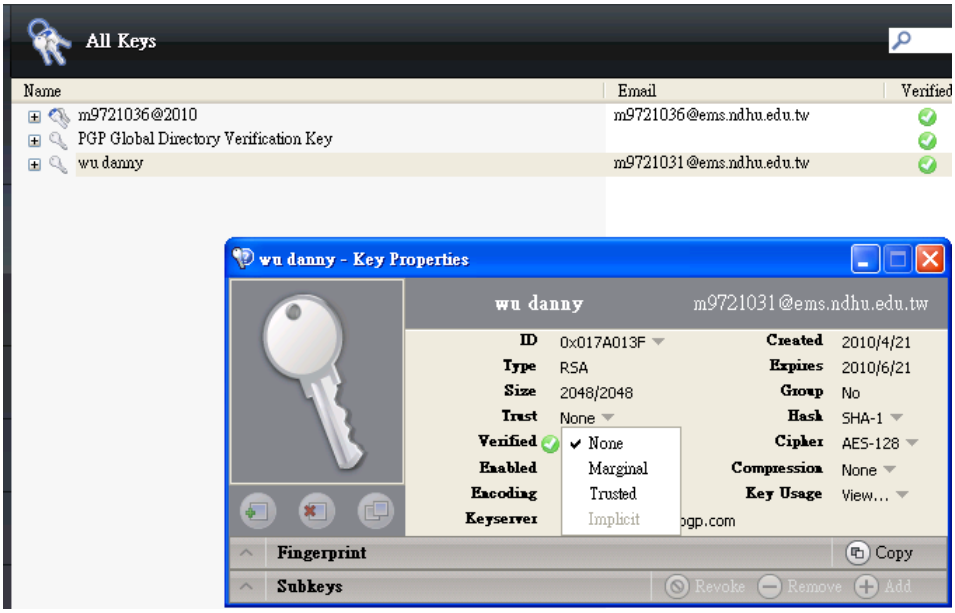
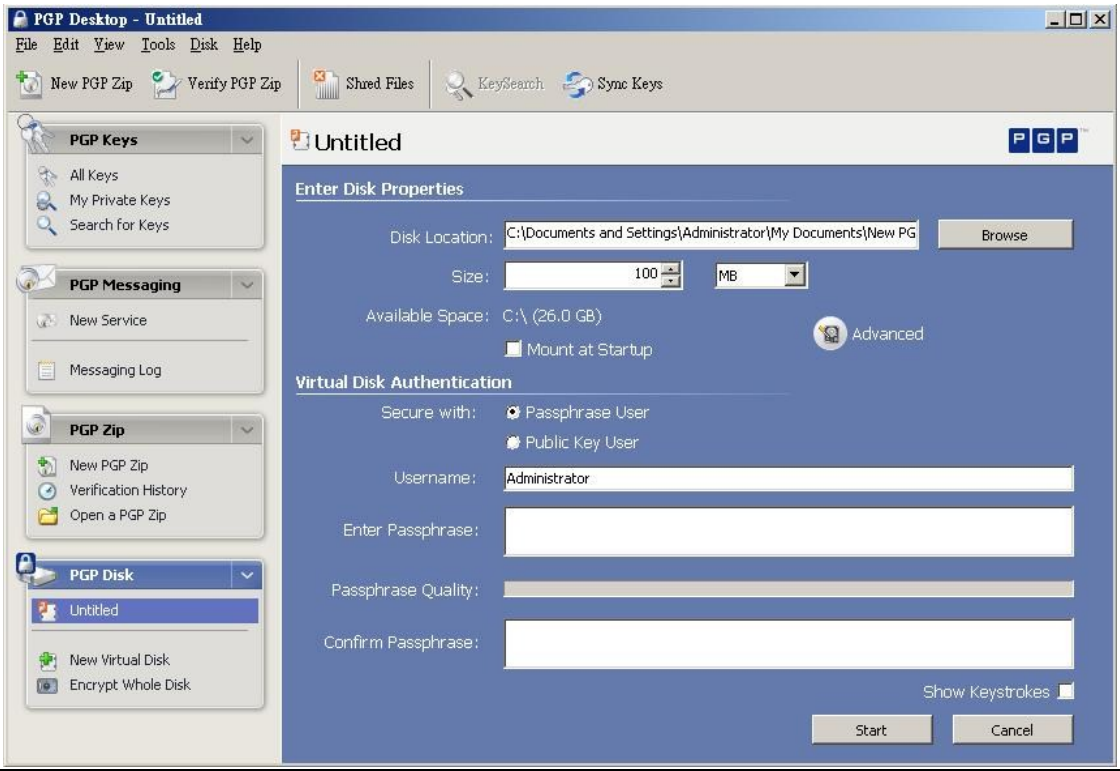
2. PGP Desktop 簡易操作

Step 1	在系統列 PGP 圖示案右鍵選擇 Open PGP Desktop 即可進到下面視窗。在此視窗我們可以看見目前在鑰匙環中的鑰匙。在鑰匙上連點兩下即可瀏覽關於鑰匙的一些資訊。 
Step 2	一開始所看到的金鑰資訊是基本的，我們可以在 View 裡勾選一些選項讓在 All Key 畫面上所顯示的資訊便多。 

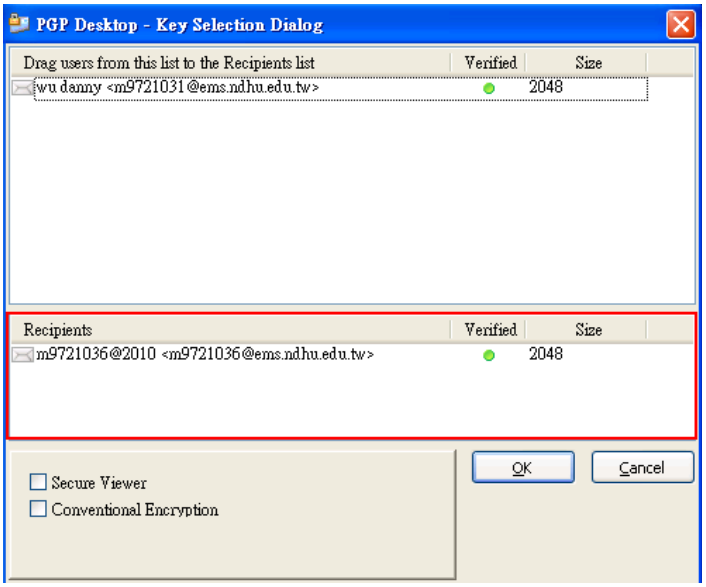
Step 3	接下來，由於預設 PGP 會將使用者的通行片語紀錄起來方便使用者不需重複輸入，但這反而會讓使用者不知通行片語的使用時機，另外也喪失了安全性，應此我們要在 Tool 裡的 Option 選項將其設定為不要紀錄通行片語。 
Step 4	若是要讓自己的公開金鑰放入鑰匙伺服器上供人搜尋下載，則在 ALL KEY 頁面上在自己的金鑰上按右鍵選擇 Send to key server 如下圖，接下來再如圖選擇下一步並輸入通行片語即可將金鑰上傳至鑰匙伺服器上。 

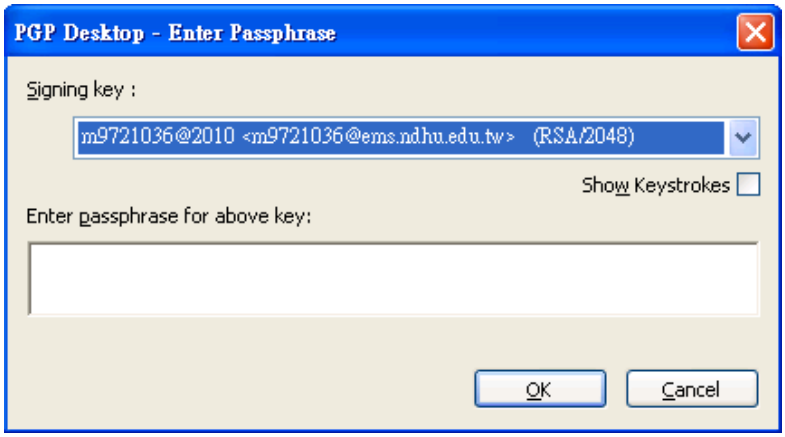
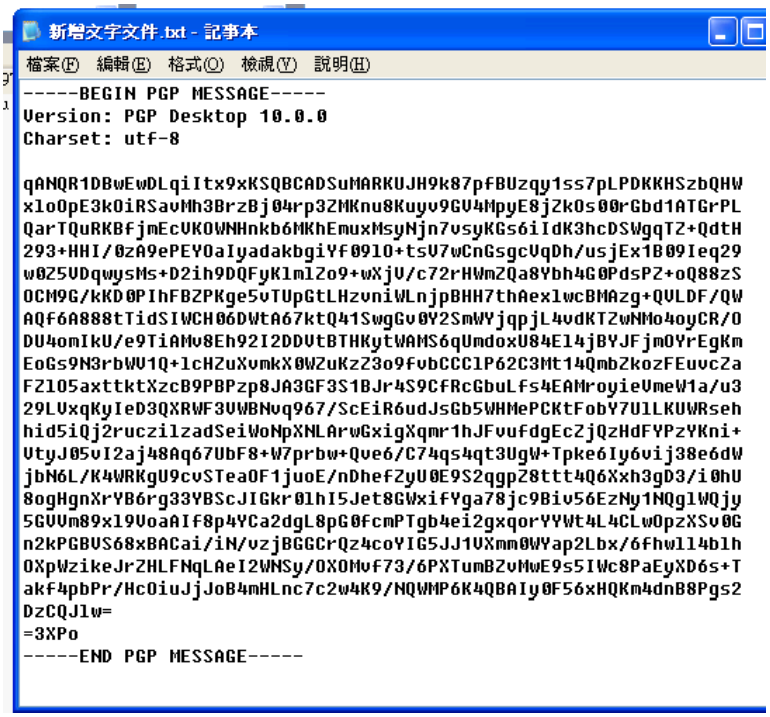
Step 5	接著我們要把別人的鑰匙加到我們的鑰匙環裡。首先選擇 search for Keys 後進到搜尋鑰匙頁面，使用者可以選擇鑰在和鑰匙伺服器，和搜尋標準後再鍵入關鍵字搜尋。搜尋到後，若要把其鑰匙加到鑰匙環中，即可在其上按右鍵選擇 add to All key。 
Step 6	加入一些 key 後即會如下圖。我們可以很清楚的看到新加入的 key 有的還未 Validate，這是為了防止有人惡意的亂加入 KEY。此外，所信任的程度也有所不同，有完全信任、半信任及不信任三種，這些都是可以手動調整的。 

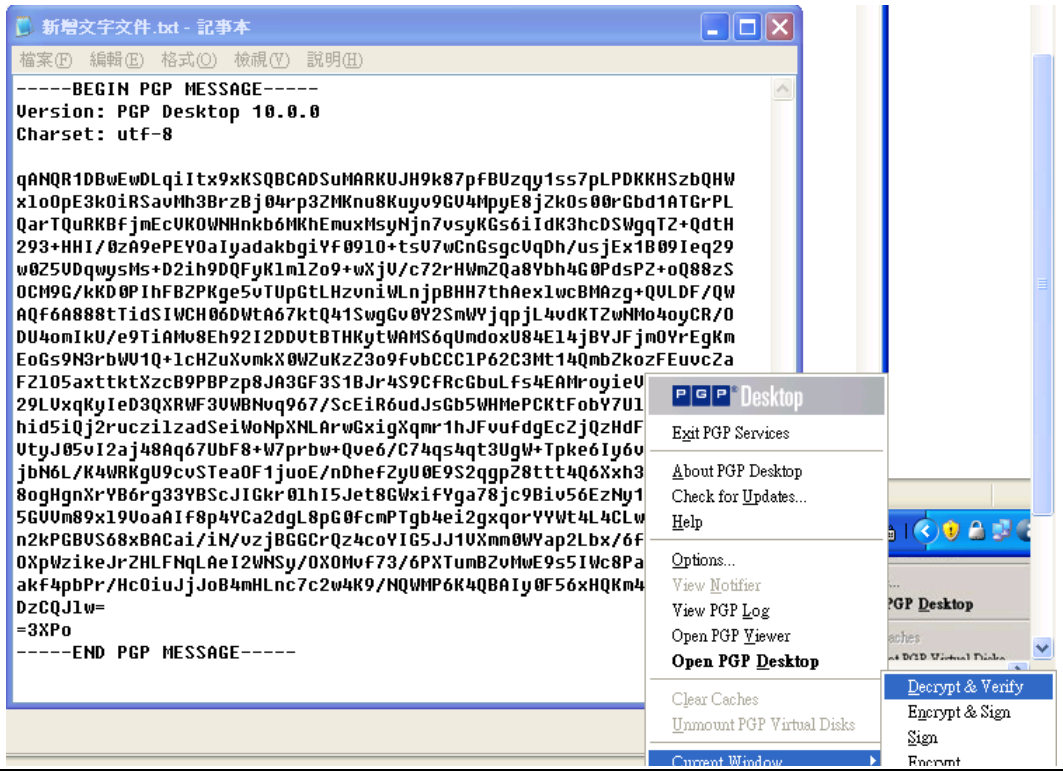
Step 7	為了要認證所新加入的鑰匙，可在欲認證的鑰匙上按右鍵選擇 Sign，接下來選擇所要 Sign 的 Key 並輸入通行片語，即可認證此把金鑰並正常使用。   

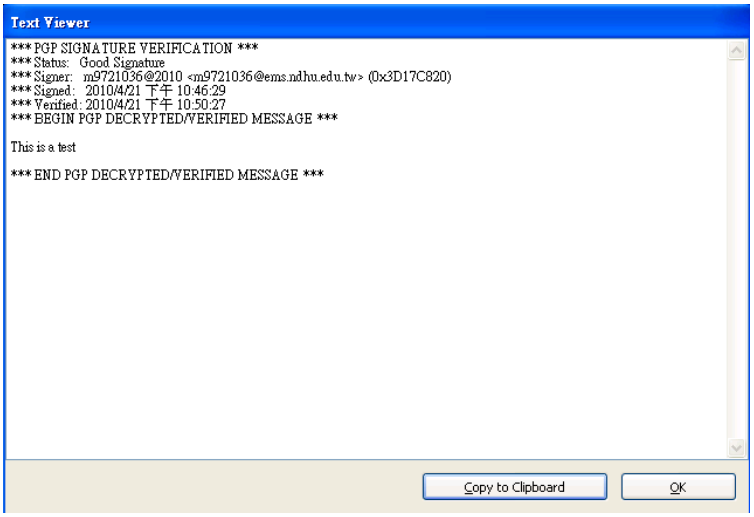
Step 8	認證完後，即可修改其信任度。修改方法為右鍵雙擊該金鑰，並在 Trust 上點選修改對其之信任度，如圖。此外由圖我們也可以看到使用者可以上傳圖片讓其他使用者更容易辨別鑰匙的主人。 
Step 9	有了對方的公開金鑰後即可開始加密資料給對方，而若雙方各有對方的公開金鑰，就可互相傳送加密文件。然而 PGP 的功能不只如此，下圖即為利用 PGP 來建立一個虛擬的硬碟，此硬碟的資料即會受到 PGP 的金鑰保護。當然此外還有許多其他的功能，本教學就不一一贅述。 

3. 基本加解密

Step 1	加密時，可開啟任一文字編輯軟體，包含 WEB Mail、WORD、等。並點選下方 PGP 圖示，選取 Current Window，選擇 Encrypt & Sign 選項加密現有文件。 
Step 2	將所要使用來加密之金鑰，由上方選擇並拖拉放置入下方選擇區。 注意！ 此加密金鑰需採用對方接收端之公開金鑰，因此需置入對方之鑰匙。 

Step 3	選擇所要用來簽章之己方個人私密金鑰，並且輸入通行片語。 
Step 4	文件加密完成後，為一 RADIX-64 文件，方便網路傳輸與應用。 

Step 5	解密時，可開啟任一文字編輯軟體，包含 WEB Mail、WORD、等。並點選下方 PGP 圖示，選取 Current Window，選擇 Decrypt & Verify 選項解密現有文件。 
Step 6	選擇解密用金鑰，並輸入對應之通行片語。 

Step 7	解密完成後之檔案。由圖可知，解回來的訊息與未加密前的訊息是一樣的，而由於加密時我們所選擇的是 Encrypt & Sign，所以上面所顯示的則是簽章的資訊。 

問題與練習：

1. 寄送加密文件時，為何需要擁有對方之公開金鑰？
2. 寄送簽章文件時，所使用的金鑰為己方或對方之私密金鑰或是公開金鑰？
3. 請實習，與友人互相寄送 **加密** 文件。
4. 請實習，與友人互相寄送 **簽章** 文件。
5. 請實習，與友人互相寄送 **簽章並加密** 文件。

總結測驗：

1. 請至 PGP Keyserver(keyserver.pgp.com)搜尋助教 A(m9921016@ems.ndhu.edu.tw)之公開金鑰，加入自己的 key ring。
2. 請至網址下載助教 B(m9921042@ems.ndhu.edu.tw)的公開金鑰，加入自己的 key ring。
3. 請將你的金鑰’ *asc’加密並簽章寄給助教 A。
4. 接收助教 A 加密並簽章的回函，解開信件內容的問題。
5. 將信件內容的答案加密(註:不簽章)送回給助教 B
6. 假設你的朋友是你 Key ring 的成員，且你對他的信賴度為 100%，若 Alice 是你這位朋友 key ring 的成員，則 Alice 加入你的 key ring 後，會被稱為有效成員。請與他組同學合作，將此實驗完成。